

## **REMARKS/ARGUMENTS**

### **1.) Claim Amendments**

The Applicant has amended claims 1, 2, 6, 13, 16-18, 25, 26, 30, 34-36, 41 and 42; no new subject matter has been added. Claims 1-11, 13-32 and 34-45 remain pending in the application.

### **2.) Examiner Objections - Claims**

The Examiner objected to claims 1, 2, 6, 13, 16-18, 25, 26, 30, 34-36, 41 for various informalities. The Applicant has amended the claims to clarify the antecedent bases of the claim elements noted by the Examiner; no substantive changes were made to the claims.

### **3.) Claim Rejections – 35 U.S.C. § 112, second paragraph**

The Examiner rejected claims 1, 25, and 41 as being indefinite on the asserted basis that "it is unclear how [the] 'determining step is done' and that "creating . . . the check token . . . based on the token secret and password' is also unclear." As previously explained, according to the principles of the claimed invention, individual authentication tokens assigned to units in a group of at least two units associated with a common password are irreversibly determined by a password; a password inputted by a user of a first unit and an authentication token of the first unit are used to determine a check token for a second unit. This is accomplished by first determining, at the first unit, a token secret using the authentication token of the first unit and the inputted password; the check token for the second unit is then created based on the token secret and the password. The check token is then sent to the second unit where it is compared with the authentication token of the second unit; if they are the same, then the user of the first device is considered authenticated. Each of those elements and functions is fully described in Applicant's specification and one of ordinary skill in the art can understand from a reading thereof how to make and practice the claimed invention. Although the specification describes exemplary processes for determining a token secret as a

function of an authentication token and a password, and for creating a check token for the second unit based on the token secret and the password, other processes can be used and are intended to be within the scope of the claims. As described hereinafter, the claims are distinguishable over the cited prior art and additional limitations are unnecessary for the invention to function as claimed. The Applicant, therefore, respectfully requests that the Examiner withdraw this basis of rejection.

#### 4.) Claim Rejections – 35 U.S.C. §103(a)

The Examiner has maintained the rejection of claims 1, 10-15, 18, 21, 25, 32-34, 37, 39, 41, 45-46, and 47 as being unpatentable over Brainard, *et al.* (U.S. Patent No. 7,363,494) in view of Schutzer (U.S. Patent Publication No. 2002/0053035); claims 12, 26 and 42 as being unpatentable over Brainard, Schutzer and Uskela (U.S. Patent No. 6,721,886); claims 3, 5, 6, 27, 29-30 and 43 as being unpatentable over Brainard, Schutzer and Hauser, *et al.* (U.S. Patent No. 5,778,065); claims 4 and 28 as being unpatentable over Brainard, Schutzer, Hauser and Aiello, *et al.* (U.S. Patent No. 6,397,329); claims 7-8, 31 and 44 as being unpatentable over Brainard, Schutzer, Hauser and Matsumoto (U.S. Patent No. 6,215,877); claim 9 as being unpatentable over Brainard, Schutzer, Hauser, Matsumoto and Gunter, *et al.* (U.S. Patent No. 6,885,388); claims 16-17, 23, 35-36 and 40 as being unpatentable over Brainard, Schutzer and Jackson, *et al.* (U.S. Patent No. 4,980,542); claims 19-20, 24, and 38 as being unpatentable over Brainard, Schutzer and MacKenzie (U.S. Patent No. 7,076,656); and claim 22 as being unpatentable over Brainard, Schutzer and McDowell, *et al.* (U.S. Patent No. 6,668,167). **The Applicant, again, traverses the rejections and rebuts the Examiner's response to Applicant's previously-submitted arguments.**

Claim 1 recites:

1. A method for password-based authentication in a communication system including **a group of at least two units associated with a common password**, comprising the steps of:  
assigning individual authentication tokens **to the respective units in the group** based on the password such that each authentication token is irreversibly determined by the password;

determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit, wherein the step of determining the check token comprises the steps of;  
determining, at the first unit, a token secret using the authentication token of the first unit and the password; and,  
creating, at the first unit, the check token for the second unit based on the token secret and the password;  
sending the check token to the second unit; and,  
comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first device is authenticated if said check token is the same as said authentication token of said second unit. (emphasis added)

The claimed invention is characterized by individual *authentication* tokens, **assigned to units in a group of at least two units associated with a common password**, that are irreversibly determined by a password. A password inputted by a user of a first unit and an authentication token of the first unit are used to determine a *check* token for a second unit. This is accomplished by first determining, at the first unit, a token secret using the authentication token of the first unit and the inputted password; the *check* token for the second unit is then created based on the token secret and the password. The *check* token is then sent to the second unit where it is compared with the *authentication* token of the second unit; if they are the same, then the user of the first device is considered authenticated. The claimed combination of elements and functions is neither taught, nor suggested, by Brainard or Schutzer, either alone or in combination.

The authentication system taught by Brainard is a conventional client-server, or monolithic, authentication system. In contrast, the Applicant's invention is directed to a distributed solution; any device can authenticate itself against any other device in the system. According to the teachings of Brainard, a user, or a group of users, can be authenticated against a central server, but they cannot be authenticated directly against other member users/devices. Using Applicants' invention, however, **a common password associated with a group of units** allows any unit to be authenticated

against another unit that is a member of a group without the need for a common authentication server, such as verification computer 450 taught by Brainard.

In responding to Applicant's arguments filed in response to the prior office action, the Examiner argues that:

Although, Schutzer was originally relied upon to show assigning individual authentication tokens to respective units in a group, **Schutzer also discloses assigning individual (i.e. unique) authentication tokens to the respective units in a group** based on a password such that each authentication token is irreversibly determined by the password on pars. 0010 or 0024-0025. (emphasis added)

As previously acknowledged by the Examiner, Brainard fails to disclose assigning individual authentication tokens to the respective units in a group. To overcome that deficiency, the Examiner has looked to the teachings of Schutzer. Schutzer does not, however, teach individual authentication tokens **assigned to units in a group of at least two units associated with a common password**. Thus, Schutzer fails to overcome the deficiencies in the teachings of Brainard.

Therefore, for the foregoing reasons, claim 1 is not obvious over Brainard in view of Schutzer. Whereas independent claims 25 and 41 recite analogous limitations, they are also not obvious in view of those references. Furthermore, whereas claims 2-11 and 13-24 are dependent from claim 1, claims 26-32 and 34-40 are dependent from claim 25, and claims 42-45 are dependent from claim 41, and include the limitations of their respective base claims, they are also not obvious over those references, or in combination with any of the further references cited by the Examiner.


\* \* \*

### CONCLUSION

In view of the foregoing amendments and remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for claims 1-11, 13-32 and 34-45.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

  
Roger S. Burleigh  
Registration No. 40,542

Date: October 5, 2009

Ericsson Inc.  
6300 Legacy Drive, M/S EVR 1-C-11  
Plano, Texas 75024

(972) 583-5799  
roger.burleigh@ericsson.com